AFRL-HE-AZ-TP-2002-0012

UNITED STATES AIR FORCE RESEARCH LABORATORY

DISTRIBUTED TRAINING NETWORK GUARD TRUSTED BRIDGE FEDERATE INITIAL CAPABILITIES DEMONSTRATION: AFTER ACTION REPORT

Richard G. Martinez

L3 Communications
6030 S. Kent Street
Mesa, AZ 85212-6061

Steven Polliard, Captain, USAF

Air Force Research Laboratory
Human Effectiveness Directorate
Warfighter Training Research Division
6030 South Kent Street
Mesa AZ 85212-6061

Robert Flo

Air Force Research Laboratory
Human Effectiveness Directorate
Information Systems Division
525 Brooks Road
Rome, NY 13441-4505

October 2002

AIR FORCE MATERIEL COMMAND
AIR FORCE RESEARCH LABORATORY
Human Effectiveness Directorate
Warfighter Training Research Division
6030 South Kent Street
Mesa AZ 85212-6061

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)
01-10-2002

2. REPORT TYPE
Interim

3. DATES COVERED (FROM - TO)
xx-07-2002 to xx-09-2002

4. TITLE AND SUBTITLE
Distributed Training Network Guard Trusted Bridge Federate Initial Capabilities Demonstration: After Action Report
Unclassified

5a. CONTRACT NUMBER
F41624-97-D-5000

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
63231F

6. AUTHOR(S)
Martinez, Richard G. ; Author
Polliard, Steven ; Author
Flo, Robert ; Author

5d. PROJECT NUMBER
4924

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
L3 Communications
6030 South Kent Street
Mesa, AZ85212-6061

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
Air Force Research Laboratory
Warfighter Training Research Division
6030 South Kent Street
Mesa, AZ85212-6061

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL; AFRL/HEA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-HE-AZ-TP-2002-0012

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES
Air Force Research Laboratory , Technical Monitor: Captain Steven Polliard, AFRL/HEA, (480) 988-6561 x-144 DSN 474-6144

14. ABSTRACT
The Air Force Research Laboratory, Warfighter Training Research Division (AFRL/HEA) located in Mesa AZ, and the Information Systems Division (AFRL/IFS) in Rome NY, in conjunction with Trusted Computer Solutions Inc. (TCS) of Herndon VA (the primary development contractor) conducted an initial capabilities demonstration of the Distributed Training Network Guard (DTNG) Trusted Bridge Federate (TBF) on 25 July 2002. The DTNG program will design and develop both a TBF and a companion Security Reclassification Rule Set Intelligent Assistant Tool (SRRSIAT). Collectively, these two components are referred to as the DTNG. The TBF is the physical real-time automated network guard component that supports two-way data transfer between simulation federations operating at different security levels. The SRRSIAT is a stand-alone interactive graphical user interface application that provides the federation security classification/domain expert with the capability to develop and review classification rules that govern the transfer of objects, attributes, interactions, parameters, and the execution of cross security level Run-Time Infrastructure operations for cross federation object models. Although the initial capabilities of the TBF were successfully demonstrated through a series of test vignettes, there were several lessons learned throughout the integration effort and the demonstration event. The hope is that the lessons will serve to improve the future demonstration.

15. SUBJECT TERMS
Distributed Training Network Guard; DTNG; Initial capabilities demonstration; Intelligent tools; Lessons learned; Networks; Security Reclassification Rule Set Intelligent Assistant Tool; SRRSIAT; TBF; Training; Trusted Bridge Federate;

16. SECURITY CLASSIFICATION OF:

a. REPORT	b. ABSTRACT	c. THIS PAGE
Unclassified	Unclassified	Unclassified

17. LIMITATION OF ABSTRACT
Public Release

18. NUMBER OF PAGES
27

19. NAME OF RESPONSIBLE PERSON
Casey, Liz
liz.casey@williams.af.mil

19b. TELEPHONE NUMBER
International Area Code
Area Code Telephone Number
480988-6561
DSN
474-6188

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39.18

NOTICES

STEVEN POLLIARD
Project Scientist

DEE H. ANDREWS
Technical Advisor

CURTIS J. PAPKE, Colonel, USAF
Chief, Warfighter Training Research Division and
Commander, Mesa Research Site

Copies of this report may be obtained from:

Defense Technical Information Center
8725 John J. Kingman Road, Suite 0944
Ft. Belvoir, VA 22060-6218
http://stinet.dtic.mil

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
October 2002

2. REPORT TYPE
Interim

3. DATES COVERED *(From - To)*
July 2002 to September 2002

4. TITLE AND SUBTITLE

Distributed Training Network Guard Trusted Bridge Federate
Initial Capabilities Demonstration: After Action Report

5a. CONTRACT NUMBER
F41624-97-D-5000

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
63231F

6. AUTHOR(S)
*Richard G. Martinez
**Steven Polliard
***Robert Flo

5d. PROJECT NUMBER
4924

5e. TASK NUMBER
B0

5f. WORK UNIT NUMBER
02

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

*L3 Communications
6030 South Kent Street
Mesa AZ 85212-6061

**Air Force Research Laboratory (AFRL)
Warfighter Training Research Division
6030 South Kent St, Mesa AZ 85212-6061

***AFRL/Information Systems Division
525 Brooks Rd, Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory
Human Effectiveness Directorate
Warfighter Training Research Division
6030 South Kent Street
Mesa AZ 85212-6061

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL; AFRL/HEA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-HE-AZ-TP-2002-0012

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
Air Force Research Laboratory , Technical Monitor: Captain Steven Polliard, AFRL/HEA, (480) 988-6561 x-144 DSN 474-6144

14. ABSTRACT
The Air Force Research Laboratory, Warfighter Training Research Division (AFRL/HEA) located in Mesa AZ, and the Information Systems Division (AFRL/IFS) in Rome NY, in conjunction with Trusted Computer Solutions Inc. (TCS) of Herndon VA (the primary development contractor) conducted an initial capabilities demonstration of the Distributed Training Network Guard (DTNG) Trusted Bridge Federate (TBF) on 25 July 2002. The DTNG program will design and develop both a TBF and a companion Security Reclassification Rule Set Intelligent Assistant Tool (SRRSIAT). Collectively, these two components are referred to as the DTNG. The TBF is the physical real-time automated network guard component that supports two-way data transfer between simulation federations operating at different security levels. The SRRSIAT is a stand-alone interactive graphical user interface application that provides the federation security classification/domain expert with the capability to develop and review classification rules that govern the transfer of objects, attributes, interactions, parameters, and the execution of cross security level Run-Time Infrastructure operations for cross federation object models. Although the initial capabilities of the TBF were successfully demonstrated through a series of test vignettes, there were several lessons learned throughout the integration effort and the demonstration event. The hope is that the lessons will serve to improve the future demonstration.

15. SUBJECT TERMS
Distributed Training Network Guard; DTNG; Initial capabilities demonstration; Intelligent tools; Lessons learned; Networks; Security Reclassification Rule Set Intelligent Assistant Tool; SRRSIAT; TBF; Training; Trusted Bridge Federate;

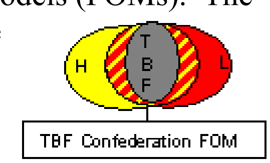
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					Ms Liz Casey
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED	27	480.988.6561 x-188 DSN 474-6188

DISTRIBUTED TRAINING NETWORK GUARD TRUSTED BRIDGE FEDERATE INITIAL CAPABILITIES DEMONSTRATION: AFTER ACTION REPORT

1.0 DISTRIBUTED TRAINING NETWORK GUARD PROGRAM BACKGROUND

1.1 Distributed Training Network Guard (DTNG) Goal/Objective: The United States Air Force has embarked on a major effort to provide the warfighter with a simulation training environment called Distributed Mission Training (DMT). The DMT network concept calls for interfacing geographically separated simulations (live, virtual, and/or constructive) into a realistic synthetic training environment to enable warfighters to "train the way they fight." However, today's distributed simulation environments can only operate at a single-system, high-security level since there are no security mechanisms to address the transfer of data between simulations executing at different security levels. That is, until completion of the DTNG Category I Advanced Technology Demonstration (ATD) program. The goal of this program is to develop a capability to allow simulation systems operating at different security levels to interoperate within a common synthetic environment thereby enhancing the capability to support full-mission training and rehearsal. More specific, the objective is to develop and demonstrate a multiple security level (MSL) network guard that supports distributed simulation training systems interoperating at different security levels within a High Level Architecture (HLA) environment. However, security practices do not typically permit direct or indirect connection between Top Secret-Sensitive Compartmented Information (SCI) and Unclassified systems. Therefore, connection of multiple single-level federation networks will likely be limited to single-step interconnections. For example, accreditation approval can reasonably be expected for connections between Top Secret-SCI to Secret-US and Secret-Releasable Levels, or between Secret-US and Secret-Releasable Levels to Unclassified.

1.2 DTNG Components/Functions: The Air Force Research Laboratory, Warfighter Training Research Division (AFRL/HEA) in Mesa AZ and the Information Systems Division (AFRL/IFS) Rome in NY, in conjunction with Trusted Computer Solutions Inc. (TCS) at Herndon VA (the primary development contractor) conducted an initial capabilities demonstration of the DTNG Trusted Bridge Federate (TBF) on 25 July 2002. The DTNG program will design and develop both a TBF and a companion Security Reclassification Rule Set Intelligent Assistant Tool (SRRSIAT). Collectively, these two components are referred to as the DTNG. The TBF is the physical real-time automated network guard component that supports two-way data transfer between simulation federations operating at different security levels. The SRRSIAT is a stand-alone interactive graphical user interface (GUI) application that provides the federation security classification/domain expert the capability to develop and review classification rules that govern the transfer of objects, attributes, interactions, parameters, and the execution of cross-security level run-time infrastructure (RTI) operations for cross-federation object models (FOMs). The TBF is designed to be FOM-independent and operates using a subset of the confederation of FOMs that include the objects and interactions that can cross security levels. The FOM associated with any specific exercise forms



the basis for all the objects and operations against which filtering and guising rules will be applied. These rules can be simple "yes/no" rules or more sophisticated rules. For example, filtering rules may be to zero out, clear, or null the data values of attributes, subattributes, parameters and subparameters. Guising or sanitizing rules allow for changing attribute or parameter values within the constraints of the data type--data type modifications will not be supported.

2.0 TBF INITIAL CAPABILITIES DEMONSTRATION

2.1 Demonstration Participants: Approximately 27 government and contractor support personnel from Air Combat Command (ACC), Aeronautical Systems Center (ASC), Naval Air Warfare Center (NAWC), Electronic Systems Center (ESC), Joint Forces Command (JFCOM), and Theater Aerospace Command and Control Simulation Facility (TACCSF) attended the TBF Initial Capabilities Demonstration event on 25 July 2002. Participants were provided an opportunity to better understand the TBF and SRRSIAT design, architecture, and functional capabilities through a series of program and technical briefings in addition to the demonstration of the TBF operating in a realistic networked simulation environment. Attachment A is a complete agenda. Feedback from the various participants was extremely positive and indicated that the DTNG program is moving forward in developing a multiple security-level capability that may not only meet the needs of the Air Force Distributed Mission Training (DMT) simulation community, but also the rest of the DoD simulation community.

2.2 TBF Functional Areas:

The TBF component consists of nine functional areas (Figure 1):

1) Rules Library;
2) Filtering and Cache;
3) Trusted Guard and Control;
4) Message Passing Interface;
5) Inbound Message Handler;
6) Outbound Message Handler;
7) Human Computer Interface (HCI);
8) Configuration Support; and
9) Auditing.

Through a series of five demonstration vignettes, eight of the nine functional areas were successfully demonstrated. The security auditing function is not yet complete. This function will record all audit entries in the Trusted Solaris, operating system, and also the TBF audit files that will be used for audit reporting and analysis. The system will audit events such as startup/shutdown, access denial, system administration activities, input/output messages, etc. Auditing is a crucial required function for security certification and accreditation. Auditing is expected to be completed by 1 November 2002.

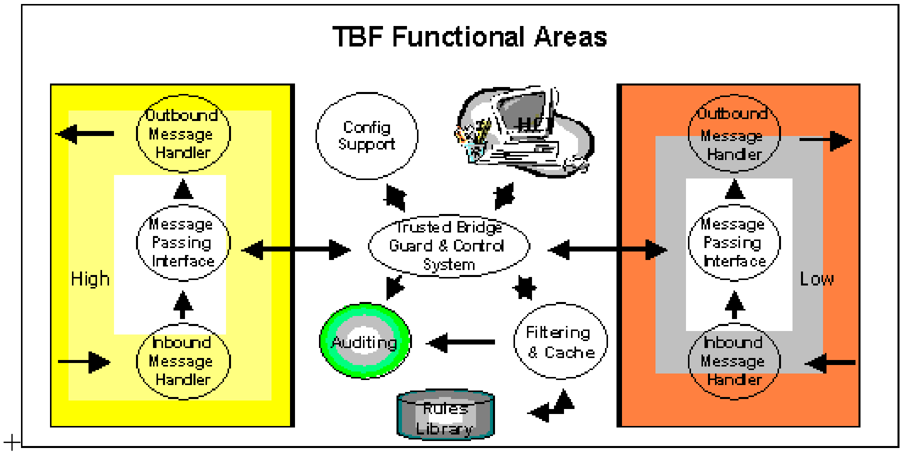


Figure 1. TBF Functional Areas

2.3. <u>Demonstration Network/Simulation Environment:</u> The TBF was integrated into the AFRL Mesa DMT test facility. A dual local area network (LAN) configuration was physically constructed to simulate the "High" and the "Low" level federations (Figure 2). The High side simulated Top Secret or Secret federates while the Low side simulated Secret or Unclassified federates, depending on the demonstration vignette. The TBF bridged the two networks and provided trusted security measures to pass information in both directions between the high and low side simulators--both networks were actually operated at the system high "Secret" security level for demonstration purposes. The simulators consisted of four F-16 Vipers, DMT Control Stations (DCSs), an Airborne Warning and Control System (AWACS) that consisted of a DCS and an Asti radio, and an Automated Threat Environment System (ATES) providing blue and red constructive forces.

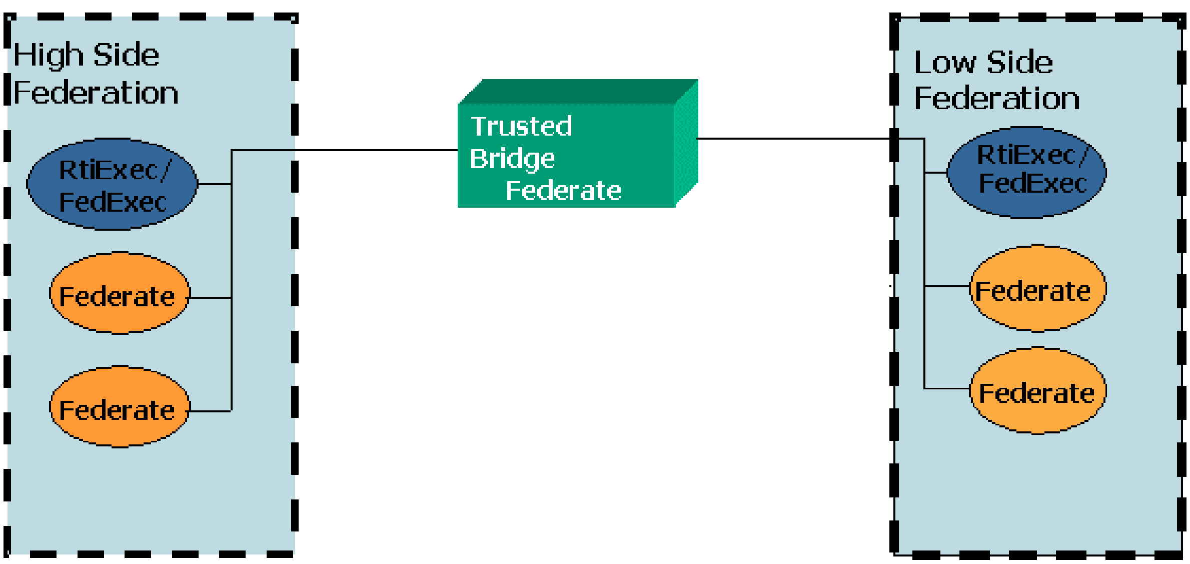


Figure 2. Demonstration Network

The simulation environment consisted of Mak Technologies HLA RTI NG 1.3.4A-NGC (for Windows) and 1.3.4A-Multi (for VxWorks), and a Nellis visual display database. The Defense Modeling and Simulation Office's (DMSO's) RTI was not used due to problems associated with the VxWorks RTI. The AFRL Mesa Network Interface Unit (NIU)/Real-time Platform Reference (RPR)-FOM 1.0 software supported the HLA environment. The TBF system configuration included a Sun Fire 880 Server with two 750 MHz CPUs each with 8 MB cache and 4 GB memory; six 36.4 GB drives, a DVD-ROM Drive, and Sun's Trusted Solaris 8.0 (04/01 evaluated release) operating system along with TCS's application software (Figure 3).

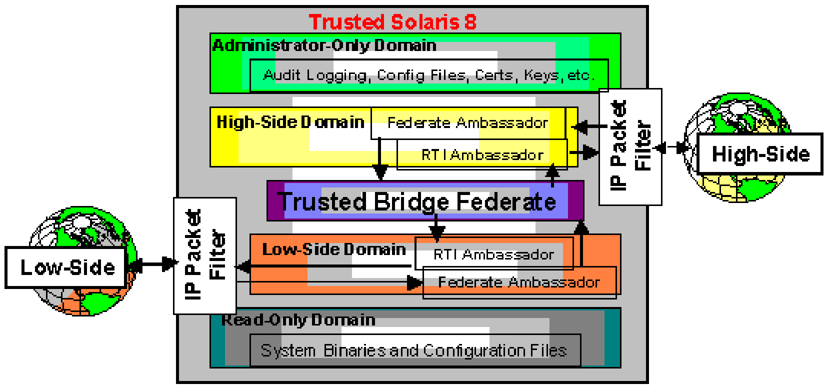


Figure 3. TBF System Configuration

2.4 Demonstration Vignettes: The TBF successfully filtered and guised the objects, attributes, and parameters specified by the rule sets. Attachment B has detailed vignette descriptions. The rule sets for the six test vignettes included 63 individual security filtering and guising rules consisting of approximately 22,758 lines of code that required three plus staff months to complete. The SRRSIAT is expected to automatically generate approximately 80% of this code when it is complete. AFRL Mesa support contractors, in conjunction with the TCS software engineers, verified at the data level that the rules were functioning as expected for all six test vignettes. However, because of time constraints and redundancy, a last-minute decision was made not to demonstrate vignette 4. During the TBF integration and pretesting, a mismatch between the new HLA Asti Radios running Mak Technologies RTI 1.3.6 and the F-16 simulators running Mak Technologies RTI 1.3.4 was discovered. This prevented an effective demonstration of voice filtering with the virtual simulators. Voice filtering was accomplished using recorded audio played through the DCSs to verify the TBF rules were functioning correctly. There was also an intermittent problem relating to the recent implementation of the RPR-FOM 1.0 NIU software that on one occasion caused a barely noticeable delay after the first missile was fired from one specific Viper. We do not believe that any of these problems were related to the DTNG TBF filtering. In all cases, the TBF filtering and guising rules worked as expected.

3.0 LESSONS LEARNED

3.1 Improvements: Although the initial capabilities of the TBF were successfully demonstrated through a series of test vignettes, there were several lessons learned throughout the integration effort and the demonstration event. The hope is that the lessons will serve to improve the future

demonstration (currently planned for November 2002). A discussion of areas where we can do things differently for better results in November follows.

Technical Interchange:

- Resolve mismatch problems between AFRL Mesa simulators running Mak 1.3.4 and the Asti Radios running Mak 1.3.6.
- Continue to ensure the NIU software implementation of RPR-FOM is matured.
- Review test vignettes to reduce network configuration changes to prevent potential problems that can be introduced with complex time-driven configuration changes.
- Review test vignettes and consolidate where possible to reduce lag-time and redundant capabilities demonstrations.
- Improve overall audio for larger audiences--look at possibility of implementing sound storm system.
- AWACS controller directions must be heard to keep audience aware the situation.
- A stealth view of important scenario situations is needed – would be ideal if we had two viewers – presentation of guising would be more effective.
- Power PC boards required for stealth viewer – investigate to see if we have resources.
- Mission map (PowerPoint) hard to see – may want to remove background map for a better view of the mission.
- DCS data values are difficult to see for large audience – continue to have mission controller (MC) explain and be prepared to freeze the scenario for closer examination.
- HLA performance in a long-haul environment is still an issue; although performance appeared very good in our limited test environment, it didn't provide much insight into performance when registering hundreds of objects.
- TCS does not have an adequate test facility – requires longer integration/testing effort at AFRL Mesa unless unclassified log files could be generated for TCS.
- Work in developing a realistic environment by installing encryption devices and routers to the overall architecture.

Schedule and Publication

- Sufficient time must be scheduled between demonstration pretesting activities and period when guests must be notified of the go/no-go demonstration decision – at least 30 days notice.
- AFRL Mesa conference room and high bay facilities will not support more than 35 participants, but more than 60 participants are expected for the November demonstration – recommend two one-day demonstration events with the first day geared toward external vendors and the second day geared toward DMT/DMO government and direct support contractors.
- Briefings and discussions flowed very well and the length of time was adequate; however, recommend a separate day for Integrated Product and Process Development (IPPD) transition discussions for November.

This page intentionally left blank.

Distributed Training Network Guard (DTNG)
Trusted Bridge Federate (TBF)
Capabilities Demonstration

AGENDA

0730: Badges/Donuts

0800: Commander's Welcome – Col Papke

0810: AFRL/HEA Overview - Dr Andrews, Tech Adv

0830: DTNG Program Overview – Capt Polliard

0900: Trusted Bridge Federate (TBF) – Mr Beskin

1000: Scenario Brief/TBF Demo 1-3 – High Bay

1130: Lunch

1240: Security Reclass Rule Set Intel Asst Tool (SRRSIAT) – Mr Beskin

1315: Scenario Brief/TBF Demo 4-6 – High Bay

1445: TBF Demo Debrief – Capt Polliard

1530: ACC/ASC IPPD Transition Discussions

This page intentionally left blank.

ATTACHMENT B

Vignette 1

Performance: Where an aircraft and/or missile's capabilities such as angle of attack, range, velocity, and acceleration must be protected as well as voice communications.

Description: Two F-22s, in this case Vipers 1 and 2 on the High side, attack a hostile target from the East releasing a High-side AMRAAM missile from a High side range. Communications between the two F-22 fighters is conducted using Asti radios set at a High-side VHF 121.5 MHZ. The AWACS and two F-16s, Vipers 3 and 4, see the F-22s as guised F-15s, on the Low side approaching the kill area from the Southeast. The two F-22s are guised by releasing an update of their position at least every 30 sec or greater and the AMRAAM missile data is not allowed to be viewed by the Low side. The AMRAAM data will not be released to the Low side with the only exception being the kill message. The target kill will be guised as an AIM-9 on the Low side so that the target can be removed from view upon kill. An F-16 will also fire at one of the hostile targets with an AIM-9 missile and all players will view the kill. F-22s are able to communicate with each other using the VHF 121.5 MHz but cannot be received by the F-16s. The F-16s can also communicate on VHF 121.5 MHz with each other and cannot be received by the F-22s. AWACS are able to observe all Low-side level data/information and able to direct both F-15s and F-16s via Asti radios over UHF 275 MHz. All players at all levels will be able to communicate over the UHF 275 MHz.

Roles:

- Vipers 1 and 2 are High-side F-22s carrying High-side AMRAAM missiles.
- Vipers 3 and 4 are Low-side F-16s carrying Low-side AIM-9 missiles.
- Asti Radios – communications system used by all Blue players.
- ATES, DCS, and an Asti radio constitute an AWACS station operating at the Low-side level.
- DCSs will be used on both the High and Low networks to view both network operations.
- ATES will provide Low-side Red air entities seen on both the Low and High sides.

Security Rules:

1. Vipers 1 and 2 (F-22s) and AMRAAM missiles to operate at the High-side level.

2. Vipers 3 and 4 (F-16s) and AIM-9 missiles to operate at the Low-side level.

3. F-22 identification will be guised as F-15s on the Low side.

    3.1. Modify Aircraft.Platform.PhysicalEntity.BaseEntity.EntityType structure data
    3.2. Modify Aircraft.Platform.PhysicalEntity.AlternateEntityType structure data
    3.3. Modify Marking string – call sign
    3.4. Strip the Aircraft.Platform.PhysicalEntity.ArticulatedParametersArray structure data out

4. F-22's position, velocity, and acceleration will be forwarded to the low side at 30 sec intervals or greater.

4.1. Pass Aircraft objects with Aircraft.Platform.PhysicalEntity.BaseEntity.EntityType of F-22 from high to low at 30-second intervals or greater. Data passed will be in accordance with numbers 3 above and 5 below.

5. F-22's angle of attack, velocity, and acceleration can be obtained directly from a single update. Therefore, these must be limited to the maximum values of an F-15.

5.1. Aircraft.Platform.PhysicalEntity.BaseEntity.AccelerationVector must be set to zero.

6. High-side missile data (fire, location, etc) will not be transmitted to the Low side. A guised kill message will be sent to the Low side so that the entity can be removed.

6.1. Do not pass WeaponsFire interactions containing WeaponsFire.MunitionType of type AMRAAM from high to low

6.2. Do not pass Munitions objects from high to low

7. The AMRAAM kill will be seen on the High side and will be guised as an AIM-9 kill on the Low side.

7.1. If the MunitionDetonation interaction contains MunitionDetonation.MunitionType of type AMRAAM

7.1.1. Change MunitionDetonation.DetonationLocation to target location else zero fields.
7.1.2. Change MunitionDetonation. FinalVelocityVector to zero.
7.1.3. Change MunitionDetonation.MunitionType from AMRAAM to AIM-9
7.1.4. Change MunitionDetonation.FuseType to zero.
7.1.5. Change MunitionDetonation.WarheadType to zero.
7.1.6. Change MunitionDetonation.RelativeDetonationLocations to zero.
7.1.7. Change MunitionDetonation.ArticulatedPartData to be zeroed out.

8. Radio communications: Only UHF 275 MHzwill be used across security levels; all other bands and frequencies will not pass between classification enclaves, such as VHF 121.5 MHz by High-side aircraft, and VHF 121.5 MHz by Low-side aircraft. AWACS will communicate on UHF 275 MHz.

8.1. There are four types of radio signal interactions; these are ApplicationSpecificRadioSignal, DatabaseIndexRadioSignal, EncodedAudioRadioSignal, and RawBinaryRadioSignal. Audio signals are passed using the EncodedAudioRadioSignal interaction. Each radio signal interaction contains a mandatory parameter called HostRadioIndex. This

parameter is used to look up the radio transmitter that issued the signal. Once the radio transmitter has been located, locate the frequency that the transmitter is transmitting on, RadioTransmitter.Frequency.

8.1.1. If the transmitter frequency equals 275 MHz, pass the signal on.

8.1.2. If the transmitter frequency does not equal 275 MHz, do not pass the signal on.

Results:

- AMRAAM launch and flyouts will only be seen on the High-side network.
- F-22 kill will be seen on High side but will appear on the Low side as an AIM-9 kill.
- AIM-9 launch flyouts and kill will be seen on both networks.
- F-16 kill will be seen on both the High- and Low-side networks.
- F-22 High-side communications will only be heard on the High side.
- Communications over UHF 275 MHz will be heard over both network areas.
- VHF communications will not cross from Low to High or High to Low.
- F-22 flight seen on High side will exhibit a smooth flight pattern while on the Low side, it will exhibit sporadic jump patterns.
- F-22 will be labeled as a F-15 on the Low side.

Vignette 2

Performance: Where an aircraft's altitude must be protected as well as voice communications.

Description: This vignette is very similar to Vignette 1 with the exception that the F-22s will be guised by protecting their altitude versus releasing their position every 30 sec. Two F-22s, in this case Vipers 1 and 2 on the High side, attack a hostile target from the East releasing a High-side AMRAAM missile from a High-side range. Communications between the two F-22 fighters is conducted using Asti radios set at a High side VHF 121.5 MHz. The AWACS and two F-16s, Vipers 3 and 4 see the F22s as guised F-15s on the Low side approaching the kill area from the Southeast. The two F-22s altitude will be restricted to 25,000 feet and the AMRAAM missile data is not allowed to be viewed by the Low side. The AMRAAM data will not be released to the Low side with the only exception being the kill message. The target kill will be guised as in AIM-9 on the Low side so that the target can be removed from view upon kill. An F-16 will also fire at one of the hostile targets with an AIM-9 missile and all players will view the kill. F-22s are able to communicate with each other but cannot be received by the F-16s, and F-16s can also communicate on VHF 121.5 MHz with each other and cannot be received by the F-22s. AWACS are able to observe all Low-side level data/information and able to direct both F-15s and F-16s via Asti radios over UHF 275 MHz. All players at all levels will be able to communicate over the UHF 275 MHz.

Roles:

- Vipers 1 and 2 are High-side F-22s carrying High-side AMRAAM missiles.
- Vipers 3 and 4 are Low-side F-16s carrying Low-side AIM-9 missiles.
- Asti Radios – communications system used by all Blue players.
- ATES, DCS, and an Asti radio constitute an AWACS station operating at the Low-side level.
- DCSs will be used on both the High and Low networks to view both network operations.
- ATES will provide Low-side Red air entities seen on both the Low and High sides.

Security Rules:

1. Vipers 1 and 2 (F-22s) and AMRAAM missiles to operate at the High-side level.

2. Vipers 3 and 4 (F-16s) and AIM-9 missiles to operate at the Low-side level.
3. F-22 identification will be guised as F-15s on the Low side.

    3.1. Modify Aircraft.Platform.PhysicalEntity.BaseEntity.EntityType structure data
    3.2. Modify Aircraft.Platform.PhysicalEntity.AlternateEntityType structure data
    3.3. Strip the Aircraft.Platform.PhysicalEntity.ArticulatedParametersArray structure data out

4. F-22s altitude will not surpass 25,000 feet. All altitudes above 25,000 will be registered at 25,000 feet.

4.1. If Aircraft.Platform.PhysicalEntity.BaseEntity.EntityType is of type F-22 and the altitude is 25,000 ft or more

4.1.1. Aircraft.Platform.PhysicalEntity.BaseEntity.WorldLocation must be set to 25,000 in the altitude direction. No actual parameter will be set to 25,000, rather the X, Y, and Z values will be adjusted appropriately to reduce the location in the altitude direction to 25000 ft. Note, the XYZ values are given in meters.
4.1.2. Aircraft.Platform.PhysicalEntity.BaseEntity.VelocityVector must be zeroed out in the altitude direction. No actual parameter will be set to zero, rather the X, Y, and Z values will be adjusted appropriately to reduce the velocity in the altitude direction to zero.
4.1.3. Aircraft.Platform.PhysicalEntity.BaseEntity.AccelerationVector must be zeroed out in the altitude direction. No actual parameter will be set to zero, rather the X, Y, and Z values will be adjusted appropriately to reduce the acceleration in the altitude direction to zero.
4.1.4. Aircraft.Platform.PhysicalEntity.BaseEntity.Orientation must be zeroed out in the pitch. Must have a pitch of zero as long as the altitude is limit locked.
4.1.5. Aircraft.Platform.PhysicalEntity.BaseEntity.AngularVelocityVector must be zeroed in the pitch direction as long as we are we are limit locked.

5. High-side missile data (fire, location, etc) will not be transmitted to the Low side. A guised kill message will be sent to the Low-side level so that the entity can be removed.

5.1. Do not pass WeaponsFire interactions containing WeaponsFire.MunitionType of type AMRAAM from high to low
5.2. Do not pass Munitions objects from high to low.

6. The AMRAAM kill will be seen on the High side and will be guised as in AIM-9 kill on the Low side.

6.1. If the MunitionDetonation interaction contains MunitionDetonation.MunitionType of type AMRAAM

6.1.1. Change MunitionDetonation.MunitionType from AMRAAM to AIM-9
6.1.2. Change MunitionDetonation.FuseType to zero.
6.1.3. Change MunitionDetonation.WarheadType to zero.
6.1.4. Change MunitionDetonation.RateOfFire to 1.
6.1.5. Change MunitionDetonation.QuantityFired to 1.
6.1.6. Change MunitionDetonation.RelativeDetonationLocations to zero.
6.1.7 Change MunitionDetonation.ArticulatedPartData to be zeroed out.

7. Radio communications: Only UHF 275 MHz will be used across security levels, all other bands and frequencies will not pass between classification enclaves, such as VHF 121.5 MHz

by High-side aircraft, and VHF 121.5 MHz by Low-side aircraft. AWACS will communicate on UHF 275 MHz.

7.1. There are four types of radio signal interactions; these are ApplicationSpecificRadioSignal, DatabaseIndexRadioSignal, EncodedAudioRadioSignal, and RawBinaryRadioSignal. They all get treated the same. Each radio signal interaction contains a mandatory parameter called HostRadioIndex. This parameter is used to look up the radio transmitter that issued the signal. Once the radio transmitter has been located, locate the frequency that the transmitter is transmitting on, RadioTransmitter.Frequency.

7.1.1. If the transmitter frequency equals 275 MHz, pass the signal on.
7.1.2. If the transmitter frequency does not equal 275 MHz, do not pass the signal on.

Results:

- AMRAAM launch and flyouts will only be seen on the High-side network.
- F-22 kill will be seen on High side but will appear on the Low side as an AIM-9 kill.
- AIM 9 launch and flyouts will be seen on both network.
- F-16 kill will be seen on both the High- and Low-side networks.
- F-22 High-side communications will only be heard on the High side.
- Communications over UHF 275 MHz will be heard over both network areas.
- VHF communications will not cross from Low to High or High to Low.
- F-22 flight seen on High side will exhibit altitudes above 25,000 feet while on the Low side, it will exhibit altitudes at 25,000 ft or below.
- F-22 will be labeled as a F-15 on the Low side.

Vignette 3

Performance: Where an aircraft and/or missile's capabilities such as angle of attack, range, velocity, and acceleration must be protected as well as voice communications.

Description: Four F-16s, in this case Vipers 1 and 2 on the High side, engage hostile targets from the West releasing High-side missiles as part of their combat engagement, while Vipers 3 and 4 also High-side aircraft, are returning from a separate strike mission and are exiting the combat area to refuel. Communications between the four High-side fighters and High-side AWACS is conducted using Asti radios on various frequencies but normally use UHF 275 MHz. The two F-16s which have exited the combat area make contact to refuel with a Low-side KC-135 tanker. Refueling communications between the F-16s, AWACS, and tanker are conducted over the Asti radios set at UHF 315.5 MHz. The KC-135 flies a track approximately 80 miles from the combat area and is unable to receive position data transmitted from the hostile targets, AWACS, or the Vipers from the High side. The AWACS is able to observe all entities' data and able to direct both F-16s and tanker for refueling via Asti radios. The KC-135 is only able to receive F-16 positions data within a 10-mile range; there are no distance limitations to radio communications. Once the F-16s are within this range, they will be picked-up on the Low-side visuals by the KC-135.

Roles:

- Vipers 1 - 4 are High-side F-16s carrying High-side missiles.
- Asti Radios – communications system used by all Blue forces.
- ATES, DCS, and an Asti radio constitute an AWACS station operating at the High-side level.
- DCSs will be used on both networks to view both network operations.
- ATES will provide High-side Red air entities.
- ATES along with an Asti radio will simulate the Low-side KC-135.

Security Rules:

1. Vipers 1 - 4 (F-16s) and missiles to operate at the High side level.
2. No missile launch, fly out, or kill data will be passed tc the Low side network
   - 2.1 Do not pass Munition class
   - 2.2 Do not pass MunitionDetonation interactions
   - 2.3 Do not pass WeaponFire interactions

3. KC-135 Tanker to operate at the Low-side level.

4. High side able to receive KC-135 data.

   4.1 Pass Aircraft class updates from low to high

5. KC-135 is able to receive all aircraft positions (Blue and Red) within a 10-mile range, except for AWACS.

5.1 If a high-side Aircraft class with an EntityType, other then AWACS, contains an Aircraft.Platform.PhysicalEntity.BaseEntity.WorldLocation attribute that is within 10 miles of the low-side tanker's Aircraft.Platform.PhysicalEntity.BaseEntity.WorldLocation, then pass WorldLocation attribute.

5.2 If a high-side Aircraft with an EntityType of AWACS, then zero out EntityType,WorldLocation, VelocityVector, AngularVelocityVector, and AccelerationVector at all times.

6. Refueling communications will only be conducted over UHF 315.5 MHz. This is the only communications allowed between the two networks. There are no distance limitations to radio communications.

   6.1 The EncodedAudioRadioSignal interaction contains a mandatory parameter called HostRadioIndex. This parameter is used to look up the radio transmitter that issued the signal. Once the radio transmitter has been located, locate the frequency that the transmitter is transmitting on, RadioTransmitter.Frequency.

   6.1.1 If the transmitter frequency equals 315.5 MHz, pass the signal on.
   6.1.2 If the transmitter frequency does not equal 315.5 MHz, do not pass the signal on.

7. Communications between F-16s and AWACS will be conducted over UHF 275 MHz and can also be conducted over various other frequencies. As per rule 6 above, only transmissions at 315.5 MHz will be allowed to cross between federations.

Results:

- Viewers on the High side able to see all entities to include KC-135.
- Viewers on the Low side will be unable to view any entities until the F-16 and/or AWACS is within a 10-mile radius.
- Refueling contact can be viewed from both the High and Low networks.
- F-16 engagement communications will only be heard on the High side.
- Communications over UHF 315.5 MHz will be heard over both network areas.

Vignette 4

Performance: Where a federation possesses a sensor whose detection mechanism must be protected.

Description: A High-side airborne radar sensor platform is able to receive electronic emissions, which are not accessible to fighter aircraft. The platform is not seen on the Low side. Four F-16s, in this case Vipers 1 - 4 on the Low side, are executing their air tasking order through a difficult corridor. Vipers have received intelligence briefing locations of known SA-6s. The High-side sensor platform has sited a new SA-xx and must immediately provide fighters with situational awareness information. The information is passed to fighters via Low-side, classified voice link--in this case, using an Asti radio over UHF 275 MHz. The information is guised and passed as the site of an SA-8.

Roles:

- Vipers 1 - 4 are Low-side F-16s carrying Low-side missiles.
- Asti Radios communications system used by all Blue forces.
- DCSs will be used on both the High- and Low-side networks to view both network operations.
- ATES will provide High- and Low-side SAs entities.
- ATES will provide the airborne radar sensor platform on the High-side network.

Security Rules:

1. Vipers 1 - 4 (F-16s) and missiles to operate at the Low-side level.

    1.1. Aircraft and Munition objects allowed to pass freely from low to high.

2. Airborne radar sensor platform to operate at the High-side level.

    2.1. Aircraft objects with Aircraft.Platform.PhysicalEntity.BaseEntity.EntityType of RC-135 are not allowed to pass their attributes from high to low. The only information allowed to pass for Aircraft of type RC-135 are: DiscoverObjectInstance, including the object name, and RemoveObjectInstance. See step 6 below.

3. The airborne sensor platform will guise all SA-xx data sent to F-16s.

    3.1. Due to a lack of available equipment, for this vignette, the sensor platform will only be able to send audio signal data. The operator must provide the declassification. The information will be sent via the EncodedAudioRadioSignal interaction. This interaction must be allowed to pass through. The EncodedAudioRadioSignal.HostRadioIndex will not be modified. The RadioTransmitter.EmbeddedSystem.HostObjectIdentifier must point to the sensor platform. No Rule needs to be written for this.

4. SA-xx emanations will not pass from the High-side to the Low-side network.

    4.1. Do not pass EmitterSystem objects
    4.2. Do not pass RadarBeam objects

5. SA-xx entities will be guised as SA-8s.

    5.1. All GroundVehicle SAM sites must have their GroundVehicle.Platform.PhysicalEntity.AlternateEntityType set to SA-8.
    5.2. Modify Markings to inusre SA-XX names are not passed
    5.3. Must zero out or otherwise remove the GroundVehicle.Platform.PhysicalEntity.ArticulatedParametersArray attribute.

6. Airborne sensor platform can only communicate (voice data) with F-16s over UHF 275 MHz.

Results:

- Viewers on the Low side will be unable to view the sensor platform.
- Viewers on the High side will be able to view all entities to include all SAs and F-16s.
- Viewers on the Low-side are unable to view SA-xx. SA-xx will appear as a SA-8.
- Communications over UHF 275 MHz will be heard over both network areas.

Vignette 5

Performance: Where a group of aircraft is able to share track and identification information that must be protected.

Description: A High-side data link, in this case, the Situational Awareness Data Link (SADL), is available to Vipers 1 and 2 on the High side. SADL provides the High-side recipients with identification information, shares data on situational intelligence information, available fuel and munitions, and is able to distinguish between foe and friendly targets. Data links are extremely important in executing close air support and receiving intelligence assets. The two other Vipers on the Low side are unauthorized the use of SADL, therefore the SADL data is unavailable to the Low side. Vipers 3 and 4, on the Low side operating without SADL, are tasked to attack a column of tanks. The two F-16s start their engagement as friendly tanks start to move towards the target (targets will be moving depending on the application providing the simulators – ATES unable to provide ground entities – JSAF able to provide moving targets). The two Vipers are able to carry out their task and exit the target area as Vipers 1 and 2, on the High side are given the authority to attack the target. Vipers 1 and 2 are able to receive target information and analyze their situation as they proceed towards the target. As Vipers 1 and 2 approach the target, they receive SADL indications that friendly tanks are now within the target area and the mission has to be aborted.

Roles:

- Vipers 1 and 2 are High-side F-16s and equipped with SADL.
- Asti Radios communications system used by all Blue forces.
- DCSs will be used on both the High- and Low-side networks to view both network operations.
- ATES will provide tanks and SAs entities.
- Vipers 3 and 4 are Low-side F-16s without SADL.

Security Rules:

1. Vipers 1 and 2 with SADL to operate at the High-side level.
2. SADL only operates with Vipers 1 and 2 and SADL data cannot be transmitted to the Low side.
3. Vipers 3 and 4 to operate at the Low-side level.
4. Communications between High- and Low-side networks can only occur over UHF 275 MHz. All other communications are isolated to classification levels.

Results:

- Viewers on the Low side will be unable to receive or view the SADL information, but are able to view Vipers 1 and 2 flight patterns and munitions.
- Viewers on the High side will be able to view all entities and the SADL information.
- Communications will only occur within the proper security levels or over UHF 275 MHz when communicating between the High- and Low-side networks.

Vignette 6

Performance: Where a group of aircraft is able to share track and identification information that must be protected.

Description: A C-130 cargo plane has been tasked to drop humanitarian supplies in a combat area and is escorted by four F-16 Vipers. The Low-side C-130 is neither equipped with radar nor able to receive Situational Awareness Data Link (SADL) information. Vipers 1 - 4 on the High side are to provide escort support, protection, and direct the C-130 to the proper drop zone. SADL provides the High-side recipients with identification information, shares data on situational intelligence information, available fuel and munitions, and is able to distinguish between foe and friendly targets. Vipers 1 and 2 on the High side are directed to a possible hostile target in the area. Vipers attack hostile target with High-side missiles, while Vipers 3 and 4 continue to the drop zone and the C-130 completes its objective. Vipers 1 - 4 are able to receive target information and analyze their situation during the entire mission while the C-130 is only able to receive Viper location data and voice communications via Asti radios over UHF 275 MHz as they proceed towards the drop zone.

Roles:

- Vipers 1 - 4 are High-side F-16s and equipped with SADL.
- Asti Radios communications system used by all Blue forces.
- DCSs will be used on both the High- and Low-side networks to view both network operations.
- ATES will provide C-130 and high-side Red entities.

Security Rules:

1. Vipers 1 - 4 with SADL to operate at the High-side level.
2. SADL only operates with Vipers 1 - 4 and data cannot be transmitted to the Low side.
3. No munitions or kill data will be sent to the Low side network from the High side.
4. Viper location data will be sent to the Low-side network.
5. C-130 to operate at the Low-side level.
6. Communications between High- and Low-side networks can only occur over UHF 275 MHz. All other communications are isolated to classification levels.
7. Mig-29 information does not get passed to the C-130.
   7.1 Do not pass aircraft object with entity type of Mig-29

Results:

- Viewers on the Low side will be unable to receive or neither view the SADL information nor missile flyouts, detonations, and kills, but are able to view Vipers 1 - 4 flight patterns.
- Viewers on the High side will be able to view all entities to include the SADL information.
- Communications will only occur within the proper security levels or over UHF 275 MHz when communicating between the High- and Low-side networks.